ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

Reliable Privacy Preserved Routing in MANET Using Backup Path

A.KAVITHA[1], E.JANITHA[2], K.DEEPIKA[3], KAVITHA.R[4]

[1]kaviashok1994@gmail.com [2]janithaezhil@gmail.com [3]petrisha01@gmail.com,

[1,2,3]UG Students, [4]Assistant Professor

[1,2,3,4] Department of Computer Science & Engineering

[1,2,3,4] Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College Avadi, Chennai.

Abstract

Mobile Ad-Hoc Networks (MANETs) are especially valuable and appropriate for discriminating situations, including military, law authorization and in addition crisis salvage and calamity recuperation. At the point when working in antagonistic or suspicious settings, MANETs oblige correspondence, security and protection in directing conventions. In many systems, where correspondence is in view of long haul personalities (addresses) the area driven correspondence worldview is more qualified for security in suspicious MANETs. In this paper, we develop an on-interest area based mysterious MANET directing convention (PRISM) Privacy amicable Routing in Suspicious MANET that accomplishes protection and security by creating reinforcement way against both outcast and insider foes. We break down the security, protection and execution of PRISM and contrast it with option strategies. Results demonstrate that PRISM is more proficient and offers preferable security over former work.

Index Terms—Privacy, communication system security,communication system routing, on-demand routing protocol, mobile communication, location-based communication, military communication.

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) assume an undeniably vital part in numerous situations and applications, particularly, in discriminating settings that need settled system framework, for example, crisis salvage, compassionate guide, and in addition military and law implementation. Since most MANETs are multi-jump in nature, coordinated and versatile steering is a significant capacity in altered systems. In the meantime, numerous MANET sending situations include operation in unfriendly situations, implying that assaults are either expected or if nothing else conceivable. In addition, dangers can begin from both outside and inside the system. While most former work in secure MANET steering concentrated on security issues, less consideration has been committed to protection. Security does not mean secrecy of correspondence (i.e., information) among MANET hubs. The recent is a central piece of secure MANET operation it is effectively accomplished by encryption, accepting that fitting key administration arrangements are utilized to set up or appropriate cryptographic keys. Protection is imperviousness to following. Since portability is the main particular MANET highlight, the arrangement of developments by a given MANET

hub can speak to delicate private data.

This is obviously not generally the situation, i.e., some MANETs don't oblige security of this sort. Though, any setting where following of MANET hubs is undesirable or hazardous would advantage extraordinarily from concealing hub developments and development designs.

Application Examples

Military and law-authorization MANETs are samples

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

of where protection, and security, is imperative . In the military case, one can envision a war zone MANET made out of diverse sorts of hubs, e.g., infantry warriors, vehicles, airplanes and different sorts of staff and gear. In the event that the enemy can track hubs developments, it can without much of a stretch derive hub types. For sample, one that moves 50 miles inside of 10 minutes is no doubt, a flying machine. Though, one moving just 5 miles inside of the same interim is presumably a vehicle. Another case in the same setting is a foe planning to track particular hubs. In the event that the enemy realizes that a certain hub compares to an administrator, it could hold up until this hub moves inside of range of expert marksman fire, with evident outcomes.

With the emphasis on security, our focal objective is to plan following safe strategies for MANETs. Such procedures can't offer a protection, since they rely on upon certain natural variables, for example, adequate system size and portability. On the off chance that hubs don't move, following resistance is plainly unthinkable. This is on the grounds that an enemy watching progressive previews of the topology can without much of a stretch see that certain hubs stay at literally the same positions. Besides, following resistance obliges us to reconsider the very essentials of MANET correspondence, e.g., how hubs allude to one another and why they impart in any case.

II. PRISM PROTOCOL

This area depicts the Privacy-accommodating Routing in Suspicious MANET (PRISM) convention. Crystal is an unknown area driven on-interest steering convention in light of three principle building hinders: (1) the understood AODV directing convention, (2) area data, and (3) any safe gathering mark plan (or one time open key endorsements).

A. AODV

AODV [12] presents an alluring establishment for PRISM, for a few reasons. AODV is on-interest (receptive) and accordingly does not proliferate topology data, conversely with proactive conventions. AODV is separation vector it doesn't return source courses (which uncover incomplete topology), not at all like source-directing based conventions. AODV is powerful since it uses flooding for course disclosure in this way, it doesn't oblige versatility to be synchronized.

B. Location centric communication

The term area driven implies that correspondence choices are made to a great extent on the premise of current topology or some other related criteria, e.g., hubs physical directions. Numerous discriminating MANET situations are not innately personality driven. Case in point, in a fiasco alleviation setting, current hub area may be substantially more critical than hub personality. There may be situations that require both area and long haul character for hubs to settle on correspondence choices. This PRISM convention utilizes the area driven correspondence.

Hit and miss approach

In the hit and miss approach a hub picks a land area (organizes), and draws a certain edge around it (e.g., by indicating a range or purposes of a polygon).It utilizes the subsequent territory as the

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

destination address. The message (course demand) tended to in such a path spreads through the system and either neglects to discover any hubs in the predefined zone or achieves one or more. Destination hub then answer utilizing state along the opposite course, with middle hubs utilizing data stored amid course demand preparing. This basic area based procedure is powerful on the grounds that, the length of the system is associated, all destinations inside of the predefined zone are come to. On the other hand, it convolutes operation since the predetermined territory may be vacant. For this situation, the source needs to either extend the edge or attempt an alternate range out and out.

C. Security

To identify the security assault to begin with, we accept a logged off Trusted Third Party (TTP). This TTP performs the elements of a Certification Authority (CA). It sets up the MANET, deals with its participation and performs different assignments, for example, measurable evaluating of security logs and afterward following of bad conduct by maverick MANET hubs (insiders).

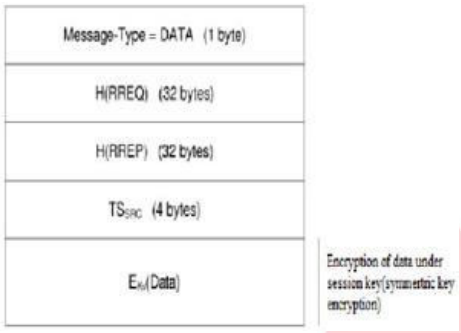
Second, we accept that, before every sending, each MANET hub has been enrolled with the TTP and has been issued fitting qualifications, for example, an open key (or a gathering mark) authentication. In the event that another hub should be added to the MANET after sending, it needs to first cooperate with the TTP to acquire its certifications. TTP obligations likewise incorporate the dissemination and administration of an all-inclusive mystery key utilized for all movement encryption. This is expected to secure against aloof outcasts who may listen stealthily on intra-MANET correspondence. We stretch that the TTP is the main party mindful of every hub's long haul character. One burden of our disconnected from the net TTP model is that individuals (hubs) must be ousted between arrangements. Thus, our security model considers dynamic insider assaults; along these lines, we shield against an acting up hub that may work inside of the MANET until the end of current sending.

Group Signatures

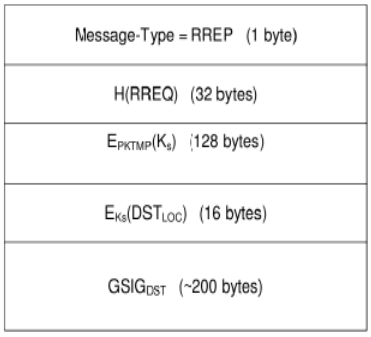
Group marks are an engaging building square for mysterious MANET directing conventions, primarily on the grounds that they fulfill the contingent protection property. Bunch marks can be seen as conventional open key marks with extra security highlights. In a gathering mark plot, any individual from a vast and element gathering can sign a message, along these lines delivering a gathering mark. A gathering mark can be confirmed by any individual who has a duplicate of a stead

Fig.1. PRISM Data Message Format

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015



(a) PRISM RREQ Message



(b) PRISM RREP Message

Fig. 1. PRISM RREQ and RREP Message Format

length group public key. A valid group signature implies that the signer is a bonafide group member. But, given two valid group signatures, it is computationally infeasible to decide whether they are generated by the same (or different) group members. Furthermore, if a dispute later arises over a group signature, a special entity called a Group Manager (GM) can force open a group signature and identify the actual signer. It is easy to imagine a group signature scheme deployed in a MANET setting, where each node corresponds to a group member and the off-line TTP corresponds to a Group Manager (GM). After route discovery, all communication between source and destination is encrypted and authenticated using a one-time (session-specific) secret key. The TTP (group manager) can later know the claimed locations of all nodes that engage in direct communication, i.e., serve as either sources or destinations. The privacy achieved by PRISM is not restricted to a specific mobility pattern.

D. Protocol Features

PRISM is designed with the following features: the source authenticates the destination and vice versa. Intermediate nodes do not know current location of the source or the exact location of the destinations. Intermediate nodes are not authenticated.

Step 2: Upon receiving a RREQ, each node firstchecks if *TSSRC* is valid. If not, the RREQ is dropped. Next, the node checks whether it has previously processed the same RREQ. This is done by computing a hash of the new RREQ (*H* (*RREQ*)) and looking it up in the local cache where all recently handled RREQ hashes are stored. Then, the node

checks whether it is within DST-AREA: (A) If not, the intermediate node caches *H*(*RREQ*) and re-broadcasts the RREQ. No RREQ fields are changed.

(B) If the node is within the destination area, it verifies *GSIGSRC*. If invalid, the RREQ is discarded. Otherwise, it stores the entire RREQ (including *GSIGSRC*). This is needed for forensic analysis, in order to identify and track misbehavior.

II. IMPLEMENTATION

The basic operation of PRISM is similar to AODV. PRISM allows a source to specify a destination area

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

and simultaneously discover multiple destination nodes in it.

Step 1: The source broadcasts a route request (RREQ)which contains the destination location, in the form of coordinates and a radius DST-AREA. RREQ also contains a temporary public key *PKTMP* , a time-stamp *TSSRC*and a group signature , *GSIGSRC*arecomputed over all previous fields. The RREQ message format is shown in Figure 1(a). The process of how the source decides to communicate and the process involved is shown in Figure 3. The source starts by searching in an area with a smaller radius and if no reply is received within a specific time window, it increases the radius of the area and sends another RREQ. A received RREP is considered to be error if the time-stamp included is incorrect, or the exact location of the replying node is not within the destination area or the verification of the group signature included in the RREP fails. In any of these cases the RREP is logged as a failing one and the source waits to receive another RREP for this RREQ.

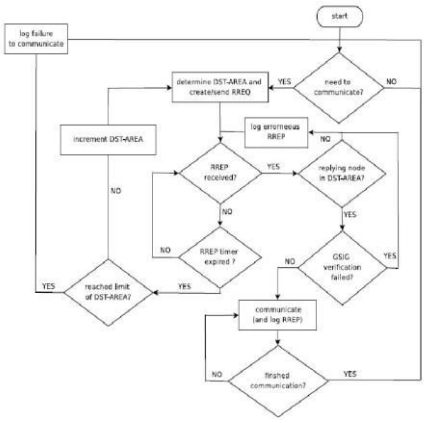


Fig.3. PRISM Sender Process

The destination then composes a route reply (RREP) which contains: (1) *H*(*RREQ*), (2) a new random session key *KS* and (3) the exact destination location. Both (2) and (3) are encrypted under *PKTMP* obtained from the RREQ. The RREP also includes the group signature *GSIGDST* of all fields. Finally, the destination broadcasts RREP. The previous sequence of operation is shown in the receiver process of PRISM in Figure 4. PRISM does not require nodes in DST-AREA to rebroadcast RREQ or to delay sending RREP in order to hide their presence.

Any insider overhearing an RREP already knows that the destination is within the area specified in the corresponding RREQ. In other words, an insider can infer from a RREP that a node exists in DST-AREA, however, it cannot learn which node. PRISM does not hide the presence of a node within a certain destination area or the fact that some node responds to a certain RREQ. It hides which node responded and prevents tracking of such nodes.

Step 3: Upon receiving a RREP, each node checkswhether it has cached the corresponding *H*(*RREQ*). If not, the RREP is dropped since this node was not on the forward route. If *H* (*RREQ*) is already cached, the node checks if the same RREP has been processed. If so, the RREP is dropped. The intermediate node now creates a new entry in its active routes table and rebroadcasts the RREP. Each active table entry contains: *H*(*RREQ*), *H*(*RREP*) and the time-stamp of entry creation.

Step 4: When the RREP is received, the source firstchecks for the correctness of the time-stamp and the exact location of the replying node then verifies the group signature.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

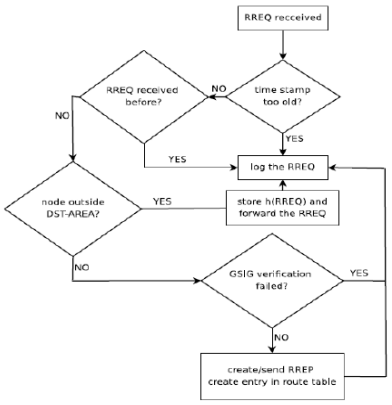


Fig.4. PRISM Receiver Process

If invalid, the RREP is discarded and logged as a failure. Next, the source decrypts the session key and location supplied bythe destination. This key is subsequently used for message encryption and/or authentication. Next, the source stores the entire RREP for forensic purposes. This completes the route set-up process shown in Figure 3. Once the route is established, each source-destination data message specifies the tuple of RREQ and RREP hashes$<H(RREQ),H(RREP)>$, as a unique route identifier. In the opposite direction, the reverse tuple ($<H(RREP),H(RREQ)>$) is used as a route identifier. The data is encrypted with the session key that was included in the RREP from the destination. Figure 2 shows the format of data messages with appropriate

field sizes. If the route breaks, a route error (RERR) message similar to that in AODV is generated.

Step 5: If the RERR message is received then thesource broadcast the RREQ message format through another route to reach the destination. This backup path is used whenever the route breaks. Hence the message can reach the destination node by the backup path.

IV. ANALYSIS

We simulate PRISM and compare it with privacy preserving location-based on demand routing protocol The goal of the simulations is two-fold: (1) to determine the routing control traffic load and required storage in PRISM, and (2) to determine how much of the network topology is leaked by PRISM.

A. Traffic Load Generated by PRISM

Figure 5 shows the average number of RREP received (both to own RREQ and those to forward) by a node. Each node periodically sends a RREQ to a random destination area. RREPs will be generated if nodes exist in that area. We see from the figure that for all mobility models, the number of RREP is always at least an order of magnitude less (sometimes even two) than privacy preserving location based on demand routing protocol. We do not show the number of RREQ sent. This number is fixed and depends on the sending rate which we determine in our simulation. In this simulation each node generates a new RREQ every 5 sec.The result is that in total PRISM will generate around 120% of the number of routing control messages of a privacy preserving location based on demand routing protocol. In such a heavy traffic scenario, where all

nodes continuously search for new destinations to communicate with, PRISM will generate slightly

more traffic overhead but will be better at hiding the topology. If only a fraction of nodes (30-50%) generate RREQs, PRISM would incur significantly less control traffic than privacy preserving location

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

based on demand routing protocol.

B. Topology Leakage in PRISM

We compare the network topology that is revealed in PRISM to that in a link-state protocol, e.g., ALARM. In link-state protocols, nodes periodically flood the entire network topology. Since a passive insider obtains successive snapshots of the entire it can violate node privacy by attempting to map nodes between adjacent snapshots. Whereas , in PRISM, in PRISM nodes do not periodically announce their locations.

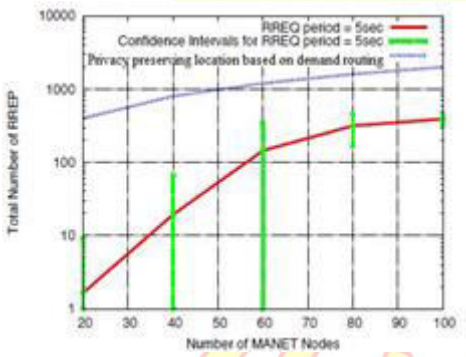


Fig .5. Routing control traffic

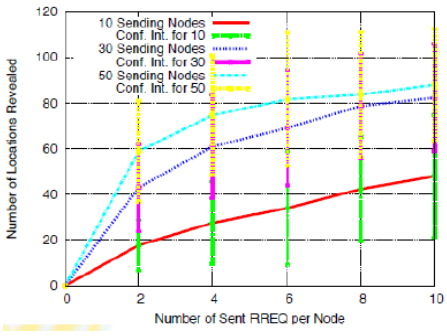


Fig.6. Network Topology Leakage

A node receiving an RREQ for a destination area where it resides, can choose not to respond if it has already responded to another RREQ within a certain window of time. The longer the window, the higher the degree of node privacy, i.e., tracking-resistance. Different packets of network topology are continuously revealed at irregular intervals. It would be very hard for a passive insider adversary to assemble them in snapshots.

V. RELATED WORK

The most relevant body of MANET research tackles secure anonymous reactive MANET routing, e.g., AO2P, ASR, ANODR, ARM, and ODAR. A survey comparing ANODR, ASR and discussing general anonymity and security issues in MANET routing protocols can be found in . Of the anonymous reactive protocols, SPAAR and AO2P require on-line location servers. ASR and ARM [16] assume that each authorized source-destination pair pre-shares a unique secret key. AnonDSR, EARP and ARMR assume that each source destination pair shares some secret information, which could be the public key of the destination or a secret key. ANODR assumes that the source shares some secret with the destination for the construction of a trapdoor, for example the destination's secret key.

SDAR [5] assumes that the source knows the public key of the destination, obtained from a certification authority (CA), and ODAR [3] requires an on-line public key distribution server. ARMR [14] utilize multiple paths for routing. It assumes that the entire network shares a pair of public private keys and that the destination ID will be encrypted under the public key. It also includes the entire path encrypted under the network key in each data message. In addition, all aforementioned

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

protocols assume that nodes know long-term identities of all other nodes, i.e., the communication paradigm is identity-centric. PRISM is fundamentally different from all prior anonymous on-demand MANET routing protocols on two accounts: (1) PRISM uses a location-centric, instead of an identity-centric, communication paradigm. Therefore, it does not assume any knowledge of long-term node identifiers or public keys. (2) PRISM requires neither pre-distributed pairwise shared secrets nor on-line servers of any kind. As an on-demand protocol, PRISM is also very different from the protocol ALARM [4], even though the latter uses group signatures and is also location-centric. ALARM is a link-state protocol and exposes the entire topology to all insiders.

VI. CONCLUSION

This paper shows the PRISM convention which bolsters unknown receptive directing in suspicious area based MANETs. It depends on gathering marks to confirm hubs, guarantee honesty of steering messages while averting hub following. It lives up to expectations with any gathering mark plan and any area based sending instrument. The reinforcement way is produced when the course disappointment happens. We assess its steering overhead and demonstrate that it can beat protection saving area based convention and unknown connection state based methodologies under certain activity designs. We likewise assess PRISM's comparing so as to follow resistance its level of topology presentation to connection state based methodologies. Crystal uncovers less of the topology and is along these lines more protection well disposed.

REFERENCES

[1] S. Seys and B. Preneel, "Arm: anonymous routing protocol for mobile ad hoc networks," Int. J. Wire. Mob. Comput.,2009, vol. 3, no. 3, pp. 145–155.

[2] E. Kumari and A. Kannammal, "Privacy and security on anonymous routing protocols in manet," in Computer and Electrical Engineering, 2009.ICCEE '09. Second International Conference on, 2009, vol. 2, 28-30 pp. 431–435.

[3] D. Sy, R. Chen, and L. Bao, "Odar: On-demand anonymous routing in ad hoc networks," Mobile Adhoc and Sensor Systems (MASS), 2008 IEEE International Conference on, Oct. 2008, pp. 267–276.

[4] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets," IEEE ICNP 2007,on Oct. 2007,pp. 304–313.

[5] A. Boukerche and K. E.-K. et al., "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks," Elsevier Computer Communications, 2005.

[6] X. Wu and B. Bhargava, "Ao2p: ad hoc on-demand position-based private routing protocol," IEEE Trans. Mobile Computing, July-Aug, 2005, vol. 4, no. 4, pp. 335–348.

[7] R. Song, L. Korba, and G. Yee, "Anondsr: efficient anonymous dynamic source routing for mobile ad-hoc networks," in SASN '05. NewYork, NY, USA: ACM, 2005, pp. 33–42.

[8] L. Kissner and D. Song, "Privacy-preserving set operations,"
CRYPTO, 2005.

[9] B. Zhu, Z. Wan, M. Kankanhalli, F. Bao, and R. Deng,

"Anonymous secure routing in mobile ad-hoc networks," Local Computer Networks, 2004,on Nov. 2004, 29th Annual IEEE International Conference on, pp. 102–108.

[10] J. Kong and X. Hong, "Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in ACM MobiHoc '03. New York, NY, USA: ACM, 2003, pp. 291–302.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

[11] S. Carter and A. Yasinsac, "Secure position aided ad hoc routing," Proc. IASTED International Conference on Communications and Computer Networks (CCN02),2002, pp. 329– 334.

[12] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM,1999, vol. 21, no. 2, pp. 120–126.

[14] Y. Dong, T. W. Chim, V. O. K. Li, S. M. Yiu, and C. K. Hui,

"Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Netw.,2009, vol. 7, no. 8, pp. 1536–1550.

[15] H. L. J. M. Xiaoqing Li and W. Zhang, "An efficient anonymous routing protocol for mobile ad hoc networks," in IAS, 2009, pp. 287– 290.

[16] PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs) by Karim El Defrawy and Gene Tsudik.